View metadata, citation and similar papers at core.ac.uk
brought to you by CORE

PolotskSU

УДК 348.3

АКТУАЛЬНЫЕ МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

канд. юрид. наук, доц. П.Л. БОРОВИК
(Академия МВД Республики Беларусь, Минск)

Рассматриваются проблемные вопросы международного противодействия преступлениям, совершаемым в сфере высоких технологий. Проведен сопоставительный анализ соответствия законодательства Республики Беларусь основным положениям Конвенции Совета Европы по борьбе с киберпреступностью, предусматривающим юридические и процедурные аспекты противодействия указанным деяниям. Сделан вывод о том, что ратификация Конвенции позволит выработать единые подходы к вопросам осуществления некоторых оперативно-розыскных и следственных мероприятий в рамках международного сотрудничества. Ряд положений, противоречащих национальному законодательству, следует учесть в соответствующих оговорках в протоколе подписания Конвенции.

Ключевые слова: *противодействие компьютерной преступности, расследование компьютерных преступлений, преступления против информационной безопасности, Конвенция Совета Европы по борьбе с киберпреступностью.*

Анализ динамики высокотехнологичной преступности позволяет утверждать, что в Республике Беларусь, как и во всем мире, по-прежнему продолжается период ее роста. Так, в 2016 году в сравнении с 2015 годом число выявленных преступлений в сфере высоких технологий увеличилось на 1,3% (с 2440 до 2471). Увеличение их количества произошло за счет прироста преступлений против информационной безопасности (глава 31 Уголовного кодекса Республики Беларусь) на 63,6% (с 404 до 651). Только количество фактов несанкционированного доступа к компьютерной информации возросло на 152,9% (с 102 до 258) [1].

Актуальность проблематики подтверждается еще и тем, что ущерб, причиняемый преступлениями в сфере высоких технологий, по разным оценкам, составляет от 150 млн до 1,1 млрд долл. США и носит высоколатентный характер. Так, по некоторым данным, в поле зрения правоохранительных органов попадает не более 10–15% всех совершаемых преступлений рассматриваемого вида [2]. Это объясняется, с одной стороны, нежеланием потерпевшей стороны (государственные, банковские и коммерческие структуры, отдельные граждане) по вполне очевидным причинам афишировать последствия, причиненные деяниями данной категории, а с другой – отсутствием определенной уверенности в наказании виновных, возврате потерянных денежных средств, возмещении ущерба и пр. Особенно это касается преступлений, совершенных с использованием информационно-коммуникационных технологий на территории нескольких государств.

Гарантировать безопасность в информационной сфере у нас в стране призваны правовые нормы, которые содержат меры ответственности за указанные правонарушения. Вместе с тем для пресечения рассматриваемых уголовно-наказуемых деяний, обеспечения безопасности критически важных объектов информатизации и иной информационной инфраструктуры разрозненных усилий отдельных государств часто бывает недостаточно. Практика противодействия современной высокотехнологичной преступности убедительно доказывает, что одной из основных ее тенденций является трансграничность, появление в ее структуре международного элемента. Поэтому очевидно, что правоохранительные органы не могут и не должны ограничиваться исключительно национальными мерами противодействия этому виду преступности. Для успешной борьбы с преступлениями в сфере высоких технологий необходимо объединение усилий всех государств, что обусловливает необходимость расширения и углубления международного сотрудничества правоохранительных органов.

Необходимо отметить, что вопросы противодействия преступлениям в сфере высоких технологий отражены в научных трудах Т.И. Абдурагимовой, Н.Ф. Ахраменки, Е.Н. Быстрякова, В.Б. Вехова, А.Д. Волеводза, Ю.В. Гаврилина, В.А. Голубева, В.С. Горбатова, О.Г. Григорьева, А.В. Касаткина, В.Е. Козлова, В.Д. Курушина, С.П. Кушниренко, В.В. Лосева, В.В, Меркушина, В.А. Мещерякова, И.Г. Мухина, А.В. Остроушко, О.Ю. Полянской, В.Ю. Рогозина, Е.Р. Россинской, Б.Х. Толеубековой, В.М. Хомича, Н.А. Швед, Н.Т. Шурухнова и др.

В работах указанных ученых затронуты проблемные аспекты международного противодействия высокотехнологичной преступности. Авторами отмечается, что преступления, совершаемые с использованием информационно-коммуникационных технологий, являются преступлениями международного характера, что предопределяет необходимость активизации международного сотрудничества в сфере борьбы с данными противоправными проявлениями. Сказанное подтверждается и мнением абсолютного большинства (100%) опрошенных нами респондентов из числа следователей и оперативных работников, специализирующихся на выявлении и расследовании рассматриваемых деяний в Республике Беларусь.

PolotskSU

Правовую основу международного сотрудничества органов внутренних дел Республики Беларусь в сфере борьбы с преступностью составляют многочисленные многосторонние и двусторонние международные договоры, заключенные на различных уровнях.

Так, в рамках Организации Объединенных Наций сотрудничество правоохранительных органов регулируется более чем двадцатью международными договорами, направленными на борьбу с торговлей людьми, незаконным оборотом наркотических средств, терроризмом, коррупцией и др.

Отношения с государствами-участниками СНГ в данной сфере регулируются межгосударственными, межправительственными и межведомственными многосторонними договорами. Кроме того, в рамках СНГ действуют соглашения о сотрудничестве в сфере борьбы с отдельными видами преступлений, в том числе и в сфере компьютерной информации [3, с. 50–52]. Между тем специфика преступлений, совершаемых с использованием информационно-коммуникационных технологий, предопределяет необходимость сбора в крайне ограниченные сроки существенного объема электронной информации из различных источников, находящихся на территории других государств. Для прослеживания маршрута движения и содержательного анализа такой информации может потребоваться ее оперативное раскрытие и сохранение, прежде чем она будет удалена. Однако существующий комплекс договорно-правовой основы международного сотрудничества не предоставляет сотрудникам оперативных подразделений Республики Беларусь правовых полномочий на поиск необходимых доказательств в соответствующей электронной среде. В свою очередь, это приводит к невозможности оперативно выявить и идентифицировать правонарушителя, совершившего (совершающего) трансграничное компьютерное преступление, а также получить доступ к его компьютеру либо используемому им серверу путем проведения «трансграничных» оперативно-розыскных и следственных мероприятий. Общепринятых же процедур сбора и раскрытия компьютерных данных зачастую бывает недостаточно. В результате, органы уголовного преследования не в состоянии оперативно реагировать на подобные виды правонарушений.

Представляется, что для преодоления растущих угроз в информационной сфере особенно важным становится принятие на национальном уровне правовой парадигмы международного сотрудничества с правоохранительными органами иностранных государств. Фундаментальным обстоятельством, определяющим успех предупреждения, выявления и пресечения преступлений в сфере высоких технологий может стать ратификация Конвенции по борьбе с киберпреступностью (далее – Конвенция), принятой Советом Европы 23 ноября 2001 года (при условии ее ратификации большинством стран мирового сообщества) [4]. В ней не только указан перечень запрещаемых действий, связанных с рассматриваемыми противоправными деяниями, но и подробно оговорены вопросы практического взаимодействия правоохранительных органов отдельных государств в ситуации, когда преступник и жертва находятся на территории разных стран и подчиняются разным законодательствам. Конвенция предусматривает конкретные механизмы, обеспечивающие эффективное и согласованное международное сотрудничество в раскрытии преступлений, связанных с использованием информационно-коммуникационных технологий.

Так, статья 14 Конвенции содержит в себе требование о необходимости законодательного и иного нормативного обеспечения использования компьютерных систем и обеспечения сбора доказательств в электронной форме при расследовании рассматриваемых преступлений.

Положения статьи 16 «Оперативное обеспечение сохранности хранимых компьютерных данных» и статьи 17 «Оперативное обеспечение сохранности и частичное раскрытие данных о потоках информации» Конвенции предоставляют возможность одной стороне добиться сохранения важной информации, необходимой для расследования преступления, которое находится в юрисдикции другой стороны. Провайдер интернет-услуг, как правило, располагает данными об информационном обмене сообщениями в прошлом, которые можно получить с помощью оборудования, регистрирующего конкретные аспекты информационного обмена, включая время, продолжительность и дату любого сообщения.

К данным сведениям относятся следующие: географическое местонахождение пользователя интернет-услуг (далее – пользователь): государство, интернет-провайдер, иная организация, а также местное время; тип средства компьютерной техники: операционная система, разрешение монитора; разработчик и версия коммуникационного программного обеспечения, при помощи которого пользователь осуществляет обращение к интернет-ресурсу; факты работы пользователя с одного и того же компьютера в данный момент и в течение предыдущего сеанса работы, а также веб-страницы или файлы, полученные из интернет-ресурсов; ссылки на эти ресурсы, использованные пользователем либо оставленные им без внимания; веб-страница, с которой пользователь знакомился до того, как попал на интернет-ресурс, и на которую перешел после этого; вопросы, формулируемые и задаваемые пользователем поисковым системам Интернета; факты шифрования компьютерной информации на участке передачи ее между компьютером пользователя и ресурсом, способы ее шифрования и получения ключей; списки почтовой рассылки пользователя, а также групп новостей, с которыми он регулярно знакомится [5, с. 64].

Указанные данные хранятся обычно в течение ограниченного периода времени, зависящего от коммерческих потребностей оператора или поставщика услуг, а также юридических требований, касающихся неразглашения частной информации. Национальное законодательство многих стран разрешает правоохра-

PolotskSU

нительным или судебным органам издавать распоряжение, касающееся сбора данных информационного обмена. В то же время в тех случаях, когда данные информационного обмена являются частью сообщения (например «заголовок» сообщений, передаваемых по электронной почте), сбор таких данных может рассматриваться как перехват самого сообщения и по этой причине подпадать под юридические ограничения [6].

Подобные требования реализованы и в национальном законодательстве. Так, в соответствии со статьей 43 Закона Республики Беларусь «Об электросвязи» от 19 июля 2005 г. № 45-З, операторы электросвязи и поставщики услуг электросвязи при взаимодействии с органами, осуществляющими оперативно-розыскную деятельность, обязаны: предоставлять в случаях и порядке, установленных законодательными актами, информацию о пользователях услуг электросвязи и об оказанных им услугах электросвязи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач; в случаях и порядке, установленных законодательными актами, оказывать содействие в проведении оперативно-розыскных мероприятий и предоставлять возможность их проведения на сетях электросвязи, принимать меры по защите сведений об организационных и тактических приемах проведения указанных мероприятий; обеспечивать в случаях и порядке, определенных законодательными актами, доступ к базам данных, автоматизированным системам; обеспечивать выполнение обязательных для соблюдения требований технических нормативных правовых актов в области технического нормирования и стандартизации, а также иных требований, установленных законодательством к сетям и средствам электросвязи, при проведении оперативно-розыскных мероприятий; выполнять иные обязанности в соответствии с законодательными актами [7].

Согласно пункту 17 Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность, утвержденного Указом Президента Республики Беларусь от 3 марта 2010 года № 129, базы данных об абонентах и оказанных им услугах электросвязи должны содержать следующую информацию: о физических лицах – абонентский номер, фамилия, имя, отчество, адрес абонента или адрес установки оконечного абонентского устройства (терминала), абонентские номера, данные, позволяющие определить (идентифицировать) абонента или его оконечное устройство (терминал), а для абонентов сети сотовой подвижной электросвязи – также реквизиты документа, удостоверяющего личность (его название, серия, номер, дата выдачи и наименование государственного органа, выдавшего документ); о юридических лицах – наименование (фирменное наименование) юридического лица, его юридический адрес, адрес установки оконечного абонентского устройства (терминала), абонентские номера, данные, позволяющие определить (идентифицировать) абонента или его оконечное устройство (терминал); общие сведения об услугах электросвязи, активированных абонентом. Указанная информация хранится оператором в соответствующих базах данных не менее пяти лет [8].

Кроме того, в соответствии со статьей 11 Закона «Об оперативно-розыскной деятельности» от 15 июля 2015 г. № 307-З организации различных форм собственности обязаны предоставлять органам, осуществляющим оперативно-розыскную деятельность, безвозмездно сведения из баз данных (учетов), информационных систем, собственниками которых они являются, путем удаленного доступа и (или) на материальных носителях информации в соответствии с соглашениями между органами, осуществляющими оперативно-розыскную деятельность, и организациями, если иное не определено законодательными актами [9].

Важными являются положения статьи 19 «Обыск и выемка хранимых компьютерных данных» Конвенции, существенно расширяющей полномочия правоохранительных органов. В первую очередь это касается правовой регламентации полномочий правоохранительных органов по оперативно-розыскным мероприятиям в отношении компьютерных систем и носителей компьютерных данных. Каждое государство обязано создать необходимые правовые условия для предоставления следующих прав и обязанностей компетентным органам по борьбе с киберпреступностью: выемка компьютерной системы, ее части или носителей; изготовление и получение копий компьютерных данных; обеспечение целостности и сохранности хранимых компьютерных данных, относящихся к делу; уничтожение или блокирование компьютерных данных, находящихся в компьютерной системе.

В статьях 20 и 21 Конвенции рассматриваются вопросы сбора компьютерных данных в режиме реального времени. Устанавливаются нормы о необходимой нормативной базе, обязывающей провайдеров проводить сбор, фиксацию и перехват необходимой информации с помощью имеющихся технических средств, а также способствовать в этом правоохранительным органам. Причем рекомендуется обязать провайдеров сохранять полную конфиденциальность о фактах подобного сотрудничества.

В статье 25 Конвенции, устанавливающей общие принципы, касающиеся взаимной международной помощи, предусмотрена возможность экстренной связи между государствами посредством электронной почты или факса. Такие сообщения должны быть защищены соответствующими средствами безопасности (включая шифрование).

В этом отношении следует отметить, в декабре 2008 года в управлении по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь при поддержке российских коллег был создан Национальный контактный пункт (далее – НКП) для координации действий с аналогичными подразделениями государств-участников группы большой «восьмерки». Данное решение позволило белорусским правоохранительным органам повысить эффективность и оперативность взаимодействия с колле-

PolotskSU

гами из 58 государств мира в деле противодействия преступлениям, совершаемым с использованием информационно-коммуникацинных технологий.

В соответствии с положениями Конвенции, каждая сторона, входящая в сеть НКП, в том числе, должна оказывать содействие любой другой стороне в обеспечении сохранности данных, хранящихся в расположенной на ее территории компьютерной системе, на срок не менее 60 дней, чтобы запрашивающая сторона могла впоследствии направить соответствующую просьбу об обыске, выемке и аналогичных действиях. На практике это означает, что после направления в зарубежное государство по каналам НКП соответствующей просьбы о сохранении информации, следователю необходимо в течение ограниченного периода времени направить в это государство международное следственное поручение для непосредственного получения необходимой информации. Возможности НКП позволяют обмениваться данными о готовящихся, совершаемых либо совершенных преступлениях, а также получать от иностранных коллег необходимые сведения для проведения оперативно-розыскных мероприятий и следственных действий.

Статья 26 Конвенции устанавливает правила, согласно которым государство может отправлять другим государствам Конвенции без предварительного запроса информацию, полученную в результате собственных исследований. Подобная практика используется в тех случаях, когда государство, отправляющее информацию, полагает, что раскрытие такой информации может быть полезно для противодействия преступлениям, совершаемых в сфере высоких технологий.

Конвенция предусматривает уголовную ответственность юридических лиц за преступления, которые совершаются в его пользу любым физическим лицом, действующим как индивидуально, так и по специальному полномочию данного юридического лица, а также вследствие ненадлежащего исполнения должностным лицом своих служебных обязанностей (ст. 12). В связи с тем, что в Уголовном кодексе Республики Беларусь не предусмотрена уголовная ответственность юридических лиц, а закреплен принцип личной виновной ответственности (ч. 1 ст. 3 УК), при подписании Конвенции положения статьи 12 должны будут осуществляться в степени, не противоречащей национальному законодательству.

Конвенция Совета Европы по борьбе с киберпреступностью также не противоречит Закону Республики Беларусь от 10.11.2008 г. № 453-З «Об основах деятельности по профилактике правонарушений». Текст Конвенции указывает на необходимость проведения в приоритетном порядке общей политики в сфере уголовного права, нацеленной на защиту общества от высокотехнологичной преступности, в том числе путем принятия соответствующих законодательных актов и укрепления международного сотрудничества.

Главным препятствием для присоединения Республики Беларусь к Конвенции являются положения статьи 32-b «Трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным», дающие иностранным спецслужбам право доступа к частным компьютерам на территории чужих государств без получения соответствующих разрешений от компетентных органов. Очевидно, что данные положения могут нанести ущерб суверенитету и национальной безопасности государств-участников Конвенции, правам и законным интересам их граждан и юридических лиц, в том числе и правам человека, таким как право на частную жизнь. Уместно заметить, что статья 32-b уже давно фигурирует в качестве «больной темы» как на европейских форумах, посвященных преступности в сфере высоких технологий, так и среди государств-участников Конвенции [10]. Поэтому вопрос о допустимости проведения указанных действий представителями правоохранительных органов на законных основаниях продолжает оставаться открытым.

Таким образом, присоединение к Конвенции Совета Европы по борьбе с киберпреступностью будет способствовать созданию препятствий для совершения преступлений рассматриваемой категории не только путем беспрепятственной идентификации правонарушителя в сети «Интернет» и установления его местонахождения в режиме реального времени с обеспечением защиты гражданских прав и свобод личности, но и выработки единых подходов к вопросам осуществления некоторых оперативно-розыскных и следственных мероприятий в рамках международного сотрудничества. Аналогичной позиции придерживаются и абсолютное большинство опрошенных нами респондентов.

Между тем совершенно очевидно, что эффективное взаимодействие субъектов уголовного преследования зависит от правовых систем их стран, а также возможности координации национальных законодательств. Следовательно, для противодействия преступности в рассматриваемой сфере всем странам необходимо гармонизировать национальное законодательство с соответствующими нормами Конвенции. Представляется, что увеличение числа участников Конвенции могло бы заложить основу универсального организационно-правового механизма международного сотрудничества правоохранительных органов.

Резюмируя вышеизложенное, сформулируем следующие **выводы:**

- одной из основных тенденций современной высокотехнологичной преступности является ее трансграничность и высоколатентный характер;

- для преодоления растущих угроз в информационной сфере особенно важным становится объединение усилий всего мирового сообщества, что обусловливает необходимость расширения и углубления практического международного сотрудничества правоохранительных органов;

- фундаментальным обстоятельством, определяющим успех предупреждения, выявления и пресечения преступлений в сфере высоких технологий может стать ратификация Конвенции Совета Европы по киберпре-

PolotskSU

ступности. Это позволит выработать единые подходы к вопросам осуществления некоторых оперативно-розыскных и следственных мероприятий в ситуации, когда преступник и потерпевшая сторона находятся на территории разных стран и подчиняются разным законодательствам. Конвенция предусматривает конкретные механизмы, обеспечивающие эффективное и согласованное международное сотрудничество в раскрытии преступлений, связанных с использованием информационно-коммуникационных технологий;

- представляется, что положения статей 12, 32-b Конвенции, противоречащие национальному законодательству, следует учесть в соответствующих оговорках в протоколе подписания Конвенции либо в заявлении об ограничении ее действия.

ЛИТЕРАТУРА

1. Статистические данные за 2016 год [Электронный ресурс] / М-во внутр. дел Респ. Беларусь. – Режим доступа: http://mvd.gov.by/ru/main.aspx?guid=3311. – Дата доступа: 10.10.2017.
2. Меркушин, В.В. Теоретико-правовые аспекты противодействия компьютерным преступлениям и иным общественно опасным деяниям в сфере высоких технологий [Электронный ресурс] / В.В. Меркушин // КонсультантПлюс. Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2017.
3. Конколович, Д.О. Договорно-правовой механизм международного сотрудничества органов внутренних дел в сфере борьбы с преступностью / Д.О. Конколович // Информ. бюл. ; ГУ «Полиграфический центр МВД Республики Беларусь». – 2013. – № 53. – С. 50–54.
4. Convention on Cybercrime [Electronic resource]. – Mode of access: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. – Date of access: 10.10.2017.
5. Козлов, В.Е. Отдельные аспекты получения криминалистически значимой информации при осуществлении противодействия компьютерной преступности / В.Е. Козлов // Вестн. Акад. МВД Респ. Беларусь. – 2016. – № 1 (31). – С. 63–66.
6. Голубев, В.А. Подписание Конвенции по борьбе с киберпреступностью и некоторые проблемы расследования киберпреступлений [Электронный ресурс] / В.А. Голубев // Центр исследования проблем компьютерной преступности. – Режим доступа: http://www.crime-research.ru/library/convention.htm. – Дата доступа: 10.10.2017.
7. Об электросвязи : Закон Респ. Беларусь, 19 июля 2005 г., № 45-З : в ред. Законов Республики Беларусь от 06.08.2007 № 277-З, от 22.12.2011 № 326-З, от 01.07.2014 № 172-З, с изм., внесенными Законом Респ. Беларусь от 30.12.2011 № 331-З) // КонсультантПлюс. Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2017.
8. Об утверждении положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность [Электронный ресурс] : Указ Президента Респ. Беларусь, 3 марта 2010 г., № 129 (в ред. Указа Президента Респ. Беларусь от 21.06.2012 № 284) // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2017.
9. Об оперативно-розыскной деятельности [Электронный ресурс] : Закон Респ. Беларусь, 15 июля 2015 г., № 307-З // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2017.
10. Постпред Рос. Федерации : Конвенция СЕ о киберпреступности – несовершенный инструмент [Электронный ресурс]. – Режим доступа: http://rus.delfi.ee/daily/estonia/postpred-rf-konvenciya-se-o-kiberprestupnostinbsp-nesovershennyj-instrument.d?id=37663167&l=fplead. – Дата доступа: 10.10.2017.

Поступила 12.10.2017

ACTUAL INTERNATIONAL LEGAL ISSUES COUNTERACTION AGAINST CRIMINALS PERFORMED IN THE SPHERE OF HIGH TECHNOLOGIES

P. BOROVIK

The article deals with the problematic issues of international counteraction to crimes committed in the sphere of high technologies. A comparative analysis of the compliance of the legislation of the Republic of Belarus with the main provisions of the Council of Europe Convention on Cybercrime, which provide for legal and procedural aspects of counteraction to these acts. It is concluded that ratification of the Convention will allow developing common approaches to the implementation of some operational search and investigative measures within the framework of international cooperation. A number of provisions that contradict national legislation should be taken into account in the relevant reservations in the protocol of signing the Convention.

Keywords: *counteraction to computer crime, investigation of computer crimes, crimes against information security, the Council of Europe Convention on Cybercrime.*